Securing Safety-Critical SCADA in the Internet of Things

Chris Johnson

School of Computing Science, University of Glasgow, Glasgow, G12 8RZ.
Johnson@dcs.gla.ac.uk, http://www.dcs.gla.ac.uk/~johnson

Keywords: Internet of Things, SCADA, Safety, Security, Industrial Control.

Abstract

In the past, industrial control systems were 'air gapped' and isolated from more conventional networks. They used specialist protocols, such as Modbus, that are very different from TCP/IP. Individual devices used proprietary operating systems rather than the more familiar Linux or Windows. However, things are changing. There is a move for greater connectivity – for instance so that higher-level enterprise management systems can exchange information that helps optimise production processes. At the same time, industrial systems have been influenced by concepts from the Internet of Things; where the information derived from sensors and actuators in domestic and industrial components can be addressed through network interfaces. This paper identifies a range of cyber security and safety concerns that arise from these developments. The closing sections introduce potential solutions and identify areas for future research.

1 Introduction

Supervisory Control and Data Acquisition (SCADA) systems support a broad range of application processes. In the past, they were localised and isolated from more conventional networks. Instead of TCP/IP, they relied on specialist protocols, including Modbus and Profibus, for vendor-neutral interfaces with a host of low-level sensors, actuators and Programmable Logic Controllers (PLCs). This situation has changed. Protocols, such as Modbus TCP/IP, offer gateways onto Industrial Control Systems (ICS). These interfaces enable the remote monitoring of distributed resources without duplicating existing network infrastructures. The PROFINET standard for industrial Ethernet provides real time extensions to TCP/IP that can be accessed through Wireless LANs. Maintenance costs are reduced, avoiding unnecessary cabling. There are also human factors benefits. Operators can use mobile controllers in a flexible manner, close to the point of need rather than being tied to a control desk. From a management perspective, enterprise planning and decision making tools can be informed by real-time process data supporting collaborative situation awareness.

Unfortunately, the cyber security of SCADA networks has not kept pace with the potential vulnerabilities that are introduced through their integration with conventional COTS networking. Many organisations have yet to adopt the International Society of Automation (ISA) cyber-security recommendation [1]. In consequence, the SHODAN search engine reveals thousands of vulnerable, misconfigured, control systems that can be accessed over TCP/IP. These vulnerabilities have numerous root causes, many of which do not stem from technical limitations. SCADA networks have been out-sourced to companies with limited experience in security- or safety-critical engineering. Tenders focus on cost reduction rather than on a risk based approach to supply-chain management.

2. The Internet of Things

These changes in the connectivity of industrial control systems have coincided with the development of the Internet of Things (IoT). This refers to physical objects – including buildings, vehicles and infrastructure components that are embedded with sensor/actuators and with processing capability, which can be addressed through network interfaces. There are strong differences between this vision and the more centralised focus of traditional ICS/SCADA networks, which by default can only be addressed within closed local area networks.

Previous paragraphs have described the erosion of such differences. This integration of SCADA and concepts from the IoT builds on earlier initiatives. For example, traditional Data Acquisition (DAQ) techniques sample the data that is necessary to optimise production processes. Most ICS applications include data historians to store and retrieve information to aid process planning and optimise manufacturing. However, the last decade has seen an opening up of what were previously closed networks as well as a transformation in the scale of integration and data exchange. For instance, SmartGrid technologies use the integration of digital networks to balance the decentralised generation and consumption of power. Similarly, 'just in time' manufacturing in next generation factories enables new levels of integration between supply and demand. The 'digital oilfield' enables operators to control massively distributed resources from a single, centralised control room.

3. Convergence of Protocols

The convergence of ICS and IoT can be traced back to common roots in Machine to Machine (M2M) protocols. These were developed to exploit real-time DAQ sources and directly informed many of the embedded, real-time infrastructures that are now being deployed in IoT enabled domestic products; including ovens, refrigerators and air conditioners.

In spite of these common roots, there are also significant differences between these SCADA techniques and the emerging IoT architectures. As mentioned, many ICS applications rely on the Modbus serial protocol. This builds on a traditional client/server model. It was originally intended to support M2M communication between Programmable Logic Controllers. In consequence, the protocol only supports data types that are recognisable by PLCs rather than the arbitrary binary objects that are envisaged within IoT architectures. A further limitation is that data objects are not transmitted with any meta-data. In other words, the semantic information needed to understand and use an object has to be embedded within each client. This limits the extensibility of Modbus networks; there are significant overheads associated with the introduction of every new node.

Modbus exploits a master/slave model. In other words, the master must explicitly poll each of the field devices. There is no way for a component to raise an asynchronous alert in response to exceptional operating conditions. Iterative polling increases the overheads associated with Modbus deployments. These constraints are exacerbated by address limitations with only 254 devices permitted on one data link. Modbus networks on their own cannot support the global connectivity envisaged in the IoT [2]. Partly in consequence, a number of alternative approaches have been developed, including those based on Message Queuing Transport Telemetry (MQTT). This is a lightweight protocol extension to TCP/IP. It avoids many of the overheads associated with Modbus by using a publish-subscribe model. Nodes must register their interest in receiving information from a publisher by contacting a broker. The protocol is also designed for low bandwidth networks and devices with limited processing capability – requiring a small code footprint. MQTT exploits a message queuing model that increases resilience in the face of different network latencies – again this is appropriate for IoT applications that must be robust to complex and dynamic environments. Amazon [3] and the US Department of Homeland Security [4] have embedded MQTT within IoT demonstrators. The DHS applications were intended to offer high levels of inherent security while enabling first responders to interact with a wide array of sensor/actuators.

Intel provide an illustration of the convergence between IoT and SCADA concepts through their integration of Modbus and MQTT in their IoT Gateways; “using Modbus as a local interface to manage devices and MQTT as a global protocol to expand the reach of those devices’ data”. In other words, their Linux-based Gateways act as an interface to conventional SCADA networks using Modbus. Data can be translated from the control domain by the Gateway into MQTT and transmitted across the Internet to distributed IoT applications. The use of TCP/IP within MQTT also helps address the scalability concerns that limit the more general application of the SCADA protocol. The combination of SCADA and IoT technologies within, for instance the new generation of Intel Gateways, provides a foundation for new levels of business integration.

4. Layers of Integration

It is possible to identify a number of different layers that are, typically, used to structure both IoT and SCADA applications:

- Business Processes: At the highest-level IoT concepts provide SCADA stakeholders with the ability to integrate diverse business processes through improved collaborative decision-making. IoT architectures have also been influenced by service-oriented architectures that support the ad hoc substitution of process components [5]. In ICS applications, it is possible to use IoT interfaces, based on the MQTT protocol, to substitute different Modbus networks if production needs to be moved between sites;

- Applications: The integration of industrial systems across both local and wide area networks provides application level control from remote locations. It also provides decision makers with multiple, real-time visualizations of underlying devices and processes that aid reporting and analysis. Not only does this support the optimisation of production processes but it also arguably helps operational staff to identify and respond to safety related concerns in a way that would not be possible if different teams relied on the manual integration of multiple data sources from individual systems, in particular where knock-on effects can propagate across chemical processes or energy distribution networks;

- Data Aggregation: The provision of application level services, in turn, depends on data aggregation. The processing and transformation of sensor data helps identify potential optimisations. Later sections will argue that the data gathered from numerous, distributed production processes can also be used to detect potential malware. For now it is sufficient to mention that the integration of SCADA into the IoT supports the deployment of big data analytics through the near real-time aggregation of distributed process information [6].

- Network Connectivity: IoT concepts and SCADA systems both depend on the deployment of network protocols that enable the real-time exchange of data

across process components. The design of these protocols has a profound impact on the scalability of the final architectures. The more information that a recipient needs to know about the sender of data then the harder it will be to substitute components or introduce novel services/devices. As we have seen, the development of ICS IoT gateways helps address the scalability problems associated with traditional SCADA protocols. However, they also raise a host of security concerns when the 'air gap' has been used to isolate industrial systems from wider Internet based applications.

- Physical Devices – there are similarities between domestic devices in the IoT and the industrial components of SCADA systems. Both make use of embedded processors. Both have significant real-time properties. However, there are also important differences – especially in terms of the kinetic forces and safety concerns that arise from potential errors or from the consequences of malware.

The following sections build on this analysis by considering the impact that different cyber-threats can have upon the safety of these different layers in the integration of ICS into the Internet of Things.

5. Case Studies and Threat Scenarios

The convergence of IoT and SCADA technologies can be illustrated smart city initiatives – such as the Sino-Singapore Guangzhou Knowledge centre taking shape in Tianjin, China. Municipal authorities are working with the suppliers of traditional ICS applications to integrate many different infrastructures [7]. These include traffic management systems; CCTV networks; weather forecasting but also power generation and management, water and heating infrastructures, revenue generation etc. The specific aims of these Smart City initiatives vary around the globe [8]. However, this integration of industrial and domestic data sources can improve air quality, reduce noise pollution and improve public safety. It can also improve resilience to the loss of infrastructure components by detecting and responding to faulty components or degraded modes of operation. Consumer data ensures 'just in time' production throughout optimised supply chains. Centralised control rooms provide stakeholders with increased levels of situation awareness that, in turn, supports cooperative decision-making.

The integration of SCADA systems within IoT and Smart City offers considerable benefits in terms of cyber security. Organisations must meet minimum standards of maturity before they can access common network and service infrastructures. The development of common gateways between the SCADA components and conventional IT networks can help to ensure consistent approaches to security – simplifying the problems of patch management and of cyber situation awareness. Ad hoc solutions to the exchange of digital data between different groups of stakeholders can lead to inconsistency and confusion about the degree of security offered at each interface.

The greater connectivity of service-oriented architectures in Smart City implementations also raises significant concerns. Most SCADA devices were designed and deployed in an era before cyber security was an explicit concern in system procurement. 'Air gaps' provided a degree of protection through isolation. Components were connected over analogue, serial circuits. The lack of external interfaces meant that attackers required physical access to the communications cables so that they could inject or exfiltrate serial data. However, the rise of IP-based communication in SCADA environments with external interfaces, for example through MQTT, means that there is no need to obtain direct physical access to an industrial control system. The integration of SCADA and IOT technologies has created and extended their mutual attack surface.

There are further concerns about individual privacy that emerge from the inclusion of SCADA applications into Smart Cities. Private companies and state agencies regularly gather data from individuals to provide statistical summaries. Statistical disclosure control (SDC) is necessary to protect individual information that might be extracted from these aggregations. IoT applications with ICS components extend the scope of data that might be collected – for example, monitoring individual power or water use to identify periods of peak capacity. The inadvertent disclosure of this data might enable criminals to target properties that were not being occupied. Location disclosing technologies, including the use of surveillance camera, are a standard feature of Smart City initiatives to both fight crime and also to optimise transportation infrastructures. However, coupled with facial recognition software they arise numerous concerns about civil liberties as well as the need to prevent unauthorised access/inferences based on the data that IoT techniques might gather to support SCADA applications [9].

Smart Cities illustrate the convergence of SCADA and IoT concepts at a macro level. Airport Operations Centres (APOCs) illustrate the same trends at a more local level. They integrate passenger and cargo operations with the airside functions that handle aircraft arrival and departure [10]. The aim is to bring together the information needed by diverse groups of stakeholders who can work together and support collaborative decision-making. For instance, Heathrow recently opened a bespoke APOC where airlines, the Air Navigation Service Provider (NATS), the UK Border Force, the Metropolitan Police and the Highways Agency share the same control room. APOCs can also combine local transportation companies, airport retailers, car park management etc. These diverse stakeholders work together to optimise the use of aircraft stands, to mitigate the impact of weather, reduce noise and environmental impact etc. As with Smart City initiatives, APOCs combine SCADA components with enterprise information systems. Baggage-handling applications, heat and lighting systems as well as air conditioning plant exploit conventional industrial control

systems. APOCs use the data provided by, for example Air Traffic Management applications, to optimise these SCADA functions.

As with Smart Cities, Airport Operations Centres raise a number of cyber-security concerns. A companion paper, in this volume [10], provides additional details. Within an APOC, it is possible to identify a number of illustrative threat scenarios. For instance, activist groups, campaigning against the expansion of an airport, might use a spear-phishing attack on junior airport management to obtain data about airport operations. They could use this to maximise the impact of direct action – for example launching runway invasions to coincide with traffic peaks or staffing shortages.

An alternate scenario involves a sub-contractor inadvertently introducing public software libraries into critical control systems. This provides a possible vector for an informed adversary to deliver a malicious payload onto IoT or SCADA infrastructures. Neither ICS protocols, such as Modbus, nor IoT infrastructures, based on MQTT, provide explicit support for the forensic analysis of cyber attacks. In consequence, there are numerous mechanisms that might support cross-infection. This would delay the detection, diagnosis and recovery from future attacks; undermining confidence in these integrated applications.

This integration of IoT and SCADA creates new concerns for cyber security and at the same time offers new hope to increase the resilience of critical infrastructures. Both the APOC and Smart City case studies support new levels of integration within integrated operations centres. The intention is to support collaborative decision-making through increased situation awareness. Most existing initiatives focus on the operational improvements and efficiency savings that are to be gained through information integration. However, it is clear that this enhanced situation awareness might also be supported by the addition of a (cyber) Security Operations Centre (SOC). The integration of multiple SCADA networks might help to identify the symptoms of coordinated or distributed attacks to multiple sub-systems. It might also provide mechanisms for tracing the root cause of a breach that might only be apparent through knock-on effects in other systems – for instance the exfiltration of SCADA production data through MQTT level interconnects. The opportunities for integrating SOCs into these initiatives has already been recognised, for instance within Law no 11/2014, establishing the Dubai Centre for E-Security [11]. Similarly, the conventional maintenance oriented network monitoring applications that have been embedded within existing APOCs are being extended to provide explicit support for the creation of Airport SOCs. Proposals have also been made to automatically feed data about potential threats to national and international SOCs for SCADA threat intelligence [12]. It remains to be seen whether such proposals can address the organisation and legal barriers that often frustrate initiatives to improve mutual cyber situation awareness.

6. Threat Mitigation

There are strong similarities between the mitigations that can be used to protect both IoT and SCADA systems. For instance, the following 'best' practices have recently been recommended for IoT implementations. It is readily apparent that they might also improve the cyber security of ICS applications [13]:

- *Best Practice 1:* Device Certificates issued to each device at the point of manufacturing to establish identity and facilitate authentication to service and other devices.

- *Best Practice 2:* As sensitive data travels through the IoT environment, it should be encrypted to prevent interception. Likewise, stored data should be transparently and seamlessly encrypted to prevent theft.

- *Best Practice 3:* Code signing of firmware/software updates using code signed with digital certificates. Additionally, all communication with devices in the field should use SSL certificates.

Unfortunately, it is non-trivial to apply these IoT recommendations to many existing SCADA networks. PLCs and sensors often lack device certification. Protocols such as Modbus do not provide any default SCADA encryption. Although this might be done at the application level, processing and bandwidth limitations in many ICS implementations mean that this recommendation is seldom followed in industrial systems, even when they interface through IoT gateways.

The encouragement to apply firmware updates and patches poses particular challenges in ICS. Traditionally, the air gap meant that isolated PLCs were seldom updated. The only way that malware might be transmitted was during a firmware update via the associated field devices. There are also more practical barriers in physically accessing devices embedded within pipelines or installed high on drilling platforms. Finally, from a safety perspective the installation of successive patches can trigger significant verification and validation costs to ensure that any changes do not violate previous requirements. Further concerns stem from the problem of ensuring that any firmware originates from a trusted source. Weak authentication schemes create concerns when safety-critical ICS devices are integrated into IoT architectures. Hash collisions enable potential attackers to make changes to authentic SCADA firmware without it necessarily being detected prior to installation on a target device.

A number of mitigations reduce the risks when SCADA systems are exposed to the IoT. Ideally, the operational domain should be physically isolated from corporate information systems. Securing the gateways between ICS and more conventional enterprise information systems can reduce the risks of cross-contamination. There are numerous techniques that can be applied – including the use of uni-

directional data diodes. Process data can be fed into decision-making tools but cyber-threats cannot be transmitted from business information systems into the more vulnerable SCADA components. However, this limits the utility of bi-directional control over massively distributed systems. What is the point in identifying complex optimisations using real-time data aggregation if the consequence control actions have to be manually communicated to each of the underlying control systems?

A more flexible approach is to use logical separation. Development and maintenance teams ensure that SCADA interfaces with IoT/IP traffic is logically separated from corporate communications and that attackers cannot exploit any potential backdoors. Logical separation can include the use of buffer networks – where SCADA systems are prevented from making any direct communication with the external Internet. If physical components of a corporate or IoT network – including routers and switches, must support the transport layer in an ICS then SCADA communications should then be encrypted and routed through VPN tunnels [14]. Within any IP-based SCADA interface to IoT applications, it is important to disable any unnecessary services and then the test that they remain disabled. Role-based access controls and authentication can limit the privileges of devices and applications to the resources they require and the principle of least privilege should contain the impact of any potential breaches. Deep packet inspection techniques may be required for protocol specific filtering to ensure that an attack does not exploit vulnerabilities within SCADA networks.

7. Conclusions and Further Work

Many existing techniques can be applied to improve cyber security at the interface between IoT technologies and SCADA applications. There are, however, particular challenges that remain to be addressed by further work. For example, it is hard to extend conventional intrusion detection systems (IDS) within safety-related applications. Black-list techniques search for the signature of known malware, by identifying associated filenames or by profiling resource utilisation. This is difficult within ICS applications where concerns over confidentiality, IPR and national sovereignty limit the exchange of malware signatures. The US ICS-Information Sharing and Analysis Centre is one of several initiatives that address these concerns. It is unclear whether the information that they provide will ever prove sufficient as a primary means of intrusion detection [15].

Alternatives rely on variants of whitelist intrusion detection. They enumerate permitted processes within a SCADA environment. Whitelisting works well in many IoT applications that do not build on legacy systems – developers and integrators can characterise those processes that are permitted to run within a system of systems. In contrast, ICS typically rely on components developed over many years. Operators seldom have access to source code or possess any deep understanding of underlying processes and resource structures. Machine learning algorithms can be used to monitor SCADA networks and identify variations from expected performance. However, these techniques cannot be used within safety-related applications because it is hard to prove that a system will not endanger safety when its behaviour changes with the training set. There are further problems with false positives – there are strong financial disincentives to halt high-integrity SCADA systems in IoT applications given the machine learning techniques often fail to distinguish degrade modes of operation from more malicious attacks. Further work is, therefore, required to develop hybrid approaches that extend IDS techniques from IoT to safety-critical SCADA environments. At present, most implementations rely on IoT level protection to prevent any intrusion inside the IDS domain and this remains a high-risk strategy as more and more operational systems are integrated within Smart City and APOC environments.

To summarise, previous generations of industrial control systems were isolated from conventional data networks. They used specialist protocols, such as Modbus and devices used proprietary operating systems. However, things are changing and industrial systems are being influenced by concepts from the Internet of Things. Information derived from sensors and actuators in production components can be addressed through network interfaces. Technical innovations, such as MQTT, provide gateways between IoT applications and SCADA systems. Higher-level enterprise management systems can exchange information to optimise and coordinate heterogeneous, massively distributed production processes. These arguments have been illustrated by case studies drawn from the integration of industrial control systems into Smart City initiatives and also Airport Operations Centres. We have then identified cyber security concerns that threaten public safety. The closing sections introduce a number of potential solutions that provide a measure of confidence in the multiple supply chains that intersect when SCADA networks are interfaced with IoT applications.

References

[1] ISA-TR99.00.01-2004 Security Technologies for Manufacturing and Control Systems, ISA-TR99.00.02-2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment, 2004.

[2] N. Mor, B. Zhang, J. Kolb, D.S. Chan, N. Goyal, N. Sun, K. Lutz, E. Allman, J. Wawrzynek, E.A. Lee, J. Kubiatowicz, Toward a Global Data Infrastructure. IEEE Internet Computing. 2016 May;20(3):54-62.

[3] Amazon, AWS IoT – Cloud Services for Connected Devices. https://aws.amazon.com/blogs/aws/aws-iot-cloud-services-for-connected-devices/. Last accessed June 2016.

[4] Department of Homeland Security, S&T's Internet of Things Pilot Demonstrates 'State of the Practical'. Last accessed June 2016.

https://www.dhs.gov/science-and-technology/blog/2016/01/25/st-internet-things-pilot-demonstrates-state-practical.

[5] H. Li, D. Seed, B. Flynn, C Mladin and R. Di Girolamo. Enabling Semantics in an M2M/IoT Service Delivery Platform. 2016 IEEE Tenth International Conference on Semantic Computing (ICSC). IEEE, 2016.

[6] Guo J, Dohler M, Kim WY, Tsoi AC, Zheng K. Mobile big data [Guest editorial]. IEEE Network. 2016 May;30(3):4-5.

[7] Electric, We Make Smart Cities a reality. Last accessed June 2016. http://www2.schneider-electric.com/documents/solutions/sustainable_solutions/Smart_Cities_Success_Stories.pdf,

[8] Y. Li, W. Dai, Z. Ming and M. Qiu, "Privacy protection for preventing data over-collection in smart city." IEEE Transactions on Computers 65.5 (2016): 1339-1350.

[9] J. Vaidya and C. Clifton, "Privacy-Preserving Data Mining: Why, How, and When," IEEE Security Privacy, vol. 2, no. 6, Nov.–Dec. 2004, pp. 19–27.

[10] C.W. Johnson, M. Shreeve, P. Sirko, O. Delain, O. Ruhlmann, E. Vautier, B. Graham and M.-T. Meloni, Defending European Airports: Cyber-Physical Threat Analysis in Total Airport Management. In IET System Safety and Cyber Security, Savoy Place, 2016.

[11] M.P. Efthymiopoulos, 2016. Cyber-security in smart cities: the case of Dubai. Journal of Innovation and Entrepreneurship, 5(1), p.1.

[12] G. Cerullo, L. Coppolino, S. D'Antonio, V, Formicola, G. Papale and B. Ragucci, 2016. Enabling Convergence of Physical and Logical Security Through Intelligent Event Correlation. In Intelligent Distributed Computing IX (pp. 427-437). Springer International Publishing.

[13] Gemalto, Securing the Internet of Things. Last accessed June 2016.http://www.safenet-inc.com/data-protection/securing-internet-of-things-iot/,

[14] H. Kim, Security and Vulnerability of SCADA Systems over IP-Based Wireless Sensor Networks, International Journal of Distributed Sensor Networks, 2012, doi:10.1155/2012/268478.

[15] C.W. Johnson, Contrasting Approaches to Incident Reporting in the Development of Security and Safety-Critical Software. In F. Koorneef and C. van Gulijk (eds.), SAFECOMP, Springer Verlag, Heidelberg, Germany, 400-409, LNCS 9337, ISBN 978-3-319-24254-5, 2015.